|  |  |
| --- | --- |
| C:\Users\lap\Desktop\imi\Без имени.pngIMI-RO  **i**nstead of **m**any **I**D - **r**egister **o**ne | Decentralized system of unified registration, identification and rating |

Appeal to the community

We live in a rapidly developing information society. Every day, hundreds of different resources appear with their own way of collecting confidential information and linking to permanent authorization. In the modern world, the life of every person is associated with a huge amount of personal documents and registration data. Since birth, many unique certificates are formed, for example – the right to drive, the right to work, eligibility for retirement, insurance, etc. Current rules force us to enter personal information for registration on sites and apps, come up with lots of names and passwords for authorization and then take cares of their safe storage. And still, even these measures do not save and sometimes lead to the abduction of data by intruders and bad consequences. However, the best way to protect them is to make them lose their value and thus cease to be interesting to outsiders. A good solution would be to replace all this set of identifiers with the one unique one, which will belong entirely only to its owner and only he can use it wherever necessary. It's time to think about this and make efforts to create one system in which you can register just once and no longer think about it, not remember many passwords, logins, access keys and other verification data. The transition to a unified system of decentralized identification, where any possibility of counterfeiting, hacking or stealing of a unique identifier will be excluded, will be a better defense of one's identity. But this can only be achieved by combining the efforts of all participants in information systems.

Let's finally change the vector of events, otherwise in the future, due to the huge pace of information development, everything will become even more complicated and more and more time will need to be spent on working with the identification, creation and storage of its unique data, logins and passwords.

All modules of the system will have open source code. Its use will be free throughout the existence of the project. And thanks to the additional decentralized relationship verification system, we can guarantee exceptional security!

Project structure

|  |  |
| --- | --- |
| C:\Users\Влад\Desktop\y-vtwPwr_3Q.jpg | Our mission  we open new horizons for information systems. |
| C:\Users\Влад\Desktop\Gj9iwsyhBzc.jpg | Our motto  is together we will make the information world easier and more reliable. |
| C:\Users\Влад\Desktop\lDJXoxXO6uA.jpg | The main method of implementing the system  is by installing the application on the device, a simple registration procedure is carried out once, as a result of which a special ID (unique identifier) is formed. The device with the ID recorded on it, becomes a unique electronic signature. All other information systems embed the second part of the App to verify the integrity of the first and extract the ID for the subsequent automatic registration and identification procedure. |
| C:\Users\Влад\Desktop\yVrKIsIP2oA.jpg | Project Objectives.   * Simplify the process of registration, identification, creation of an electronic signature and electronic certification as much as possible. * Draw attention of a community ready for change! All those who do not want to create more and more new IDs for themselves, and then entrust their storage to u outsiders and systems. * Make the user rating formation and storage voluntary, reliable and not substitute. * Fundamentally change existing approaches and methods of implementing procedures for the protection of all information resources. |
| C:\Users\Влад\Desktop\73XNvuJAlds.jpg | Role of the project  to make all information systems easier and safer. |
| Development Strategy – to pass 5 stages: | |
| C:\Users\Влад\Desktop\4wEC0z4VBqY.jpg | Aveloni  public involvement in the issue of unified registration and identification, analysis of opinions with their subsequent structuring. Identification of key factors for adjusting the direction of the development vector. Analysis of the capabilities of DIDs methods and other open similar projects; |
| C:\Users\Влад\Desktop\MPjD1usATws.jpg | Biatrini  before writing application codes, verification module and blockchain, testing and publishing on all open resources; |
| C:\Users\Влад\Desktop\he5u_nvILLg.jpg | Ciatri  development and promotion of these technologies; |
| C:\Users\Влад\Desktop\PzLEk4n2Uvs.jpg | Daciri  enter personal ratings into the system, such as:   * credit * social * labor * and others   and their safe use in all information systems; |
| C:\Users\Влад\Desktop\ogSqGJ4dTVQ.jpg | Frigeli  recognition by the society and the transition to a single decentralized system of identification and rating. |
| C:\Users\Влад\Desktop\v3Y8QEor6Jg.jpg | Key Approach  not the client adjusts to the service, but the service adjusts to the client! |
| C:\Users\Влад\Desktop\e0KSuxCuJf8.jpg | Values.   * Confidentiality and security of data storage. Important personal information should be kept exclusively by the owner of the personal data. * Time. It will not be necessary to spend a lot of time completing various registrations and storing a large amount of personal IDs. * Decentralized approach. Additional program protection against code modification to counterfeit an electronic signature. |
| C:\Users\Влад\Desktop\OPoLHSqbVB0.jpg | Functions.   * Generation of an electronic signature without having to visit the certification centre and pay related services. * Ability to link all existing documents that appear in the process of a person's life to a decentralized ID. * Use of the same user identification in all information systems. * KYC “Know Your Customer” procedures for APP, DAPP and DeFi. * Additional modules can be connected if desired. |
| C:\Users\Влад\Desktop\pA3DKf3f7jk.jpg | Road map.  AVE – until 07.01.2022  BIA – until 20.12.2023  CIA – until 03.10.2025  DAC – until 01.11.2025  FRI – until 10.10.2026  Postponements are possible if there is a lack of funding. |
| C:\Users\Влад\Desktop\NS5JyP9-NLM.jpg | Block chain token   * token name - IMI * number of tokens - 20 Billion * yield on staking 20% * function 1 - storage of verification keys * function 2 - voting in the project * distribution 20% - the project team, 30% - sales at the AVE stage, 50% - sales at the BIA stage. |
|  | Architecture |
| C:\Users\Влад\Desktop\EDXHZO1pFUY.jpgC:\Users\Влад\Desktop\0PYd1_Yk-6k.jpg | Implementation  Anyone at the time of purchasing an electronic device, using a decentralized IMI-RO application having an Internet connection, will conduct an initial registration to record their electronic signature (ID) in a special memory location of the device. This cell will be arranged in such a way that after writing a unique ID into it, it will go into the "lifetime" mode - "read-only." This will eliminate any possibility of changing, deleting and overwriting it - which will also reduce the number of fraudulent transactions.  When registering, you will need to enter the following data – Last name, First name and patronymic, date of birth and Pin code - 4 digits. After that, using a special irreversible hash function, an ID set to long will be created, which in the future will be the key to all systems and the electronic signature of the owner.  The IMI blockchain, using hashing techniques and verification keys, will recognize the integrity of the program that attempts to write the ID into the device cell. If successful, it recognizes the combination of ID and the Device identical and, having formed its own "Success" code, will record it in its log, otherwise it will publish the coordinates of the device on suspicion of fraud.  Further, all registration, identification and authentication procedures will take place quickly and invisibly for the user. At the hardware level, this will be implemented according to the following scheme:  In addition to its identification system, each developer will build a system for verifying the originality of the IMI-RO App, codenamed ARLISIA. It will check the client IMI-RO code, and if it is not fake, it will consider his ID and authorize the user under it. If the outcome is negative, it will send the device coordinates to the IMI blockchain for further publication in the list of suspicious devices. |
| C:\Users\Влад\Desktop\jyJj0-BOJQA.jpg | Additional features.   * The device memory cell will be designed so that only the IMI-RO module can write or read data from it and have two types: * The ID cannot be changed or deleted after recording, in which case there are no procedures for transferring the device. It is the safest option. * The device transfer procedure can be used no more than 3 times. Less secure type. * The IMI-RO App and the ARLISIA module will have open source and will be available absolutely free of charge to all users of the system on open resources. * For organizations, the procedures will be similar, and have their own additional features, submodules and concept, which will be published closer to the beginning of the second stage. |
| C:\Users\Влад\Desktop\JeRIrNyy3M8.jpg | Emergency situations  if attackers stole the device or obtained remote access to it, the PC-IMI technique will be used. |
| C:\Users\Влад\Desktop\xEQzygOk6Qs.jpg | BIA Planned Modules  • PC-IMI technique  • IMI-RO and ARLISIA interaction monitoring system, checking the correctness of trust relationship setting  • Scalability Analyzer. |
| C:\Users\Влад\Desktop\8Y56-X5iyCY.jpg | The economic component  part of the funds that are now spent on the development and support of the identification systems will be used to ensure the safe functioning of the IMI blockchain. The rest of the costs that information systems now incur to protect against attacks will be used to develop their core functions. |
| C:\Users\Влад\Desktop\v8WQ99nToSQ.jpg | Document variability  is a project of the system that is under development and will be modified and supplemented in the development process. The description of the project is ultimately simplified as well as the purpose of the project - to make working with information systems FASTER and EASIER. |
| The current version of the project is - 1.0 |
| C:\Users\Влад\Desktop\71Z-7vQw190.jpg | Anti Plagiarism – some of the descriptions may overlap with Decentralized Identifiers (DIDs) v1.0 – https://www.w3.org/TR/did-core/and Self-Sovereign Identity SSI. – https://ec.europa.eu/futurium/en/system/files/ged/eidas\_supported\_ssi\_may\_2019\_0.pdf  The implementation is different from the presented developments.  If you believe that Copyright ideas, realizations or rights are used in this project, please write to reg@imi-ro.pro.  Based on the results of analysis and negotiations, we will definitely take this into account in the further development of IMI-RO. This document is copyrighted. And any of its contents cannot be used for commercial purposes. |

Authors and main project participants:

|  |  |  |  |
| --- | --- | --- | --- |
| C:\Users\lap\Desktop\imi\я.png | Leschinskiy Alexander  Age – 36 years old  Financial University,  Direction: business informatics | C:\Users\Admin\OneDrive - sucden.ru\Рабочий стол\дапп\Иван.png | Sheremetov Ivan  Age – 31 years old  Industrial and Technological College,  Technician-mechanic |
| C:\Users\Admin\OneDrive - sucden.ru\Рабочий стол\дапп\Миша.png | Migunov Mikhail  Age – 28 years old  Financial College,  Economist | C:\Users\Admin\OneDrive - sucden.ru\Рабочий стол\дапп\димка.png | Dmitry Golubev  Age – 24 years old  Agrarian University,  Direction: Agroengineering |
| C:\imi\photo_2021-10-06_12-45-30.jpg | Makhmudov Ruslan  Age – 30 years old  Technical university,  Engineer technologist | C:\imi\photo_2021-10-06_13-45-22.jpg | Olga Nekrasova  Age – 34 years  Pedagogical university;  Philologist |
| C:\Users\Admin\OneDrive - sucden.ru\Рабочий стол\дапп\артем.png | Ivanov Artyom  Age – 40 years  Vladimir Dahl National University,  Direction: Flexible Computer Systems and Robotics | C:\imi\Без имени.png | Kirkin Roman  Age – 29 years old  Pedagogical University  Direction: technologies and methods of information protection. |